REMARKS/ARGUMENTS

Claims 13-18 and 20-44 are currently pending in the present application. Based on the following remarks, Applicant requests reconsideration of the application and allowance of the claims.

I. Rejection of Claims 13-18 & 20-44 Under 35 U.S.C. § 103(a)

Claims 13-18 and 20-44 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Roke Manor Research Limited (GB #2 349 548A; hereinafter "Roke Manor") in view of Red Fig Limited (GB #2 344 491A; hereinafter "Red Fig") and Halpern et al. (U.S. Patent No. 6,282,711; hereinafter "Halpern").

Claim 13, requires a client-server system comprising, *inter alia*, a client terminal and a remote server. The client terminal includes a portable radio communication device including a user interface and authentication means. The user interface comprises a plurality of user selectable menu applications and a browser application which operates to request *content,* which *comprises validation* data *and other* data, *stored at the server*. One or more of the menu applications has embedded therein, a sub-menu containing a user selectable direct download link comprising an address of the server. In response to a user selection of the direct download link from the sub-menu, the browser application controls the radio communication device to transmit a signal to connect to the server. The authentication means comprises a means for checking the validation data of the content downloaded from the server, and the remote server comprises means for *downloading the content* to the portable radio communication device *with the validation data* so as to be *identifiable* by the authentication means *as originating from the server*. The *validation data and the other data* are downloaded from *the server together* in a *single download file*. Applicant respectfully submits that the combination of Roke Manor, Red Fig and Halpern does not teach or suggest at least the above recitations of claim 13.

Contrary to the Examiner's assertion, the process of authentication in Roke Manor is such that software is received from one place such as the broadcaster 14 and then the authentication code is received from another place such as the network operator 12. In contrast to the Examiner's assertion if some other entity (e.g., a non-originating server) has the correct authentication code, this authentication code may very well be sent from this other entity (e.g., non-originating server). Claim 1 recites that the content comprises validation data and other data that is stored at *the server* (a single device) and that the authentication means of the client terminal comprises a means for checking the validation data of the content that is downloaded from the server so as to be identifiable by said authentication means as originating from the server. The combination of Roke Manor, Red Fig and Halpern do not teach or suggest this feature of claim 13. Rather, as pointed out above, the system of Roke Manor can be a compromised (cracked) system in that there could be a vigilante server sending cracked authentication codes to telecommunications devices 16. And furthermore, the software and the authentication code of Roke Manor are sent from different devices, namely the broadcaster 14 and the network operator 12, whereas claim 13 recites that the content comprises the validation data and other data which is stored at *the server* (i.e., a single entity) and is downloaded from *the server* (i.e., a single entity). For at least these reasons, the combination does not teach or suggest all of the features of claim 13.

Additionally, in rejecting claim 13, the Examiner correctly concedes Roke Manor and Red Fig, alone or in combination do not teach or suggest "wherein the validation data and the other data are downloaded from the server together in a single download file," as claimed. However, the Examiner relies on Halpern to make up for the deficiencies of Roke Manor and Red Fig. Applicant disagrees and submits that Halpern does not make up for what Roke Manor and Red Fig lack. Applicant submits that nowhere in Halpern, alone or in combination with Roke Manor and Red Fig, (and the Examiner cites to none, in fact the Examiner cites to no section of Halpern) is there any mention, teaching or suggestion relating to any validation data that is downloaded from a server where the validation data is checked by an authentication means so as to be identifiable as originating from a server, as required by claim 13. Rather, Halpern, at best, discloses that a user may customize an installation package at a server and explains that the installation package "contains only the programs, data, … local installation tools" and "options requested by the user during a dialog with the server" and describes that this installation package is sent to the client system 101. (Col. 4, lines 44-50 & Abstract of Halpern) Halpern is simply altogether silent regarding any download of validation data from a server to a client terminal being validation data that originated with the server, as claimed. In this regard, claim 13 determines whether the download of the content is from a trusted server. (See pg. 10, lines 23-30 of the specification) As known to those skilled in the art, a trusted server is one which a portable radio communication device recognizes as a server authorized to provide content to the portable radio communication device which may be on the basis of information downloaded to the portable communication device. (See *id.*) In this regard, claim 13 provides a safeguard against the content crashing the portable radio communication device. (See *id.*) Since Halpern as well as the other references, each fail to teach or suggest the download of the claimed validation data, the combination is deficient and claim 13 is patentable for at least this reason. To the extent that the Examiner persists in this rejection, Applicant respectfully requests the Examiner to specifically point out in Halpern where Halpern allegedly discloses download of the claimed validation data, as the current rejection does not cite to any column, line number or Figure in Halpern.

Applicant points out that in rejecting claim 13, the Examiner continues to suggest that the authentication code of Roke Manor corresponds to the claimed validation data and suggests that the software of Roke Manor corresponds to the claimed other data. (See number 2. on pg. 2 of the Office Action) Additionally, the Examiner suggests that the network operator 1 of Roke Manor corresponds to the claimed server.

In actuality, Roke Manor, at best, discloses that the software (alleged other data) is broadcast from broadcaster 14 and then in a subsequent and entirely separate transmission, the authentication code (alleged validation data) is transmitted from the network operator 12, to the device 16, via GSM base station 18, so that the previously broadcast and received software (alleged other data) can be enabled. Contrary to the Examiner's assertions, Roke Manor, at best, discloses that the software (alleged other data) and the authentication code (alleged validation data) are downloaded to the device 16 separately in two different transmission steps and at two different times. First, the software is delivered to and received by the device 16. Then the device 16 contacts the network operator 12 and "[t]he network operator 12 then [i.e., subsequently] "transmits an authentication to the subscriber 16, which enables the … software to run." (pg. 4, lines 13-15 of Roke Manor) As such, the software is received at the device 16 by itself, i.e., without the inclusion of the authentication code in its data stream. The authentication code is sent, by the network operator 12, during a different and subsequent transmission step, i.e., after the device 16 initiates a point to point connection and contacts the network operator 12.

In contrast, to Roke Manor, Halpern, at best, discloses that the components and options selected by the user are sent to the client system 101 in an installation package via a server. Since the network operator 12 of Roke Manor sends the software to the device 16 and another device such as broadcaster 14 transmits the authentication code to a base station which then sends the authentication code to the device 16, modification of the network operator (alleged server) of Roke Manor such that both the software and the authentication code are sent from the network operator 12 (alleged server) to the device 16 changes the principle of operation of Roke Manor and there is no reasonable expectation that the references can be successfully modified in the manner suggested by the Examiner. And as such the proposed combination violates the mandates set forth in MPEP §§ 2143.01, 2143.02.

Based on at least the foregoing reasons, Applicant submits that the combination of Roke Manor, Red Fig and Halpern is deficient and does not teach or suggest all of the features of claim 13. Applicant therefore respectfully requests the Examiner to reconsider and withdraw the § 103(a) rejection of claim 13 and it dependent claims 15, 16, 23, 25, 30, 35 and 40.

Since claims 14, 17, 18 and 20 contain features that are analogous to, though not necessarily coextensive with, the features recited in claim 13, Applicant respectfully submits that claims 14 and 17 and their respective dependent claims 21, 22, 24, 26, 31, 36, 41 and 27, 32, 37 and 42 as well as independent claims 18 and 20 and their respective dependent claims 28, 33, 38, and 43 as well as claims 29, 34, 39, and 44 are patentable at least for reasons analogous to those submitted for claim 13.

With further regard to claims 25-29, Applicant submits that claims 25-29 recite independently patentable subject matter. In rejecting claims 25-29, the Examiner relies on Roke Manor as disclosing these features. (See pg. 5 of the Office Action) Contrary to the Examiner's general allegation, Roke Manor, at best, discloses that the subscriber of device 16 selects the service, e.g., software that he/she is interested in using and in response, the device listens for the software and when the software is detected the "software is downloaded and installed" on the device 16. Subsequently, the subscriber may request the authentication code from the network operator to enable the software previously installed on the device 16. (pg. 6, lines 11-17 & pg. 4, lines 10-15 of Roke Manor) Nowhere in the combination is there any teaching or suggestion that the authentication code identifies the network operator or a server, as set forth by Claims 25-29.

The combination is altogether silent regarding the nature of the information pertaining to the authentication code. The authentication code could simply be a key to enable the software without specifying any information identifying a server or the network operator 12. Further, since the software is installed on the device 16 prior to being enabled by the authentication code, the combination does not teach or suggest that the authentication code (i.e., alleged validation data) indicates to the authentication means whether the software and the authentication code (alleged content) is accepted by the device 16, as claimed. For at least the foregoing reasons, Applicant respectfully requests the Examiner to reconsider and withdraw the § 103(a) rejection of dependent claims 25-29 for the additional reasons discussed above.

Regarding claims 30-34, Applicant submits that claims 30-34 recite independently patentable subject matter. (See pg. 5 of the Office Action) In rejecting claims 30-34, the Examiner relies on Roke Manor. Applicant disagrees. As noted above, since Roke Manor describes that the software is installed on device 16 and is subsequently enabled by the authentication code, Applicant submits that the combination fails to teach or suggest that the software (alleged other data) is rejected by the authentication means if the authentication means determines from the authentication code (i.e., alleged validation data) that the authentication code and software (alleged content) did not originate from *the server*, as required by dependent claims 30-34. The software of Roke Manor is not rejected by the device 16 since it is installed on device 16 before being enabled by the authentication code. Nowhere in the combination is there any teaching or suggestion that the authentication code identifies whether the software and the authentication code (alleged content) did not originate from the network operator or the same server, as claimed. Claims 30-34 require that "the content is rejected … if the authentication means determines from the validation data that the content did not originate from the server" and the combination does not teach or suggest this feature. In this regard claims, 30-34 facilitate blocking of downloaded content from unauthorized sources such as unauthorized servers. (See pg. 10, lines 23-25 of the specification) For at least these additional reasons, Applicant respectfully requests the Examiner to reconsider and withdraw the § 103(a) rejection of dependent claims 30-34.

Concerning claims 35-39, Applicant submits that claims 35-39 recite independently patentable subject matter. In rejecting claims 35-39, the Examiner again relies on Roke Manor.

Applicant disagrees. Given that Roke Manor describes that the software is installed on device 16 prior to being enabled by the authentication code, as described above, Applicant submits that the combination is incapable of teaching or suggesting that the content is *installed* on the device 16 *after* the content is *validated* by the authentication means as originating from the server, as required by claims 35-39. Roke Manor, alone or in combination with Red Fig and Halpern, at best, discloses that the software is installed on the device 16, and may subsequently be enabled. As such, Applicant respectfully requests the Examiner to reconsider and withdraw the § 103(a) rejection of dependent claims 35-39 for the additional reasons discussed above.

With further regard to claims 40-44, in the Amendment filed April 25, 2007, Applicant pointed out that claims 40-44 are independently patentable given that the combination of Roke Manor, Red Fig and Halpern fails to teach or suggest "wherein the validation data and the other data are downloaded concurrently from the server," as claimed. In rejecting claims 40-44, Applicant relies on Red Fig as disclosing these features. Applicant disagrees and points out that the Examiner relied merely relied on Red Fig as allegedly disclosing the claimed browser application and relied on Roke Manor as allegedly disclosing the claimed validation data, the claimed other data and the claimed server. As noted above, Roke Manor in combination with Red Fig and Halpern, at best, discloses that the software is downloaded and received by the device in a first data stream. Then the device 16 initiates a point to point contact with the network operator and the authentication code is subsequently transmitted in a second data stream so that the previously received software can be enabled. The software and the authentication code of the combination are transmitted to the device 16 at different times and different instances. As such, Applicant again submits that the combination fails to teach or suggest that the software (alleged other data) and the authentication code (alleged validation data) are downloaded from the server concurrently, as required by claims 40-44. Applicant therefore respectfully submits that the dependent claims 40-44 are patentable at least for this additional reason.

Moreover, Applicant notes that the Examiner has not responded to the arguments set forth above and specifically at pg. 13 of the Amendment filed on April 25, 2007. However, MPEP § 707.07(f) requires that "[w]here the [A]pplicant traverses any rejection, the [E]xaminer should … take note of the [A]pplicant's argument and answer the substance of it." In contrast to the requirements of MPEP § 707.07(f), the Examiner has not responded to Applicant's arguments. To the contrary, the grounds of rejection merely contains the sweeping assertion that Red Fig discloses "validation data and the other data are downloaded concurrently from the server" without citing to any page, paragraph, column, line number, Figure, etc. and without providing any substantive explanation whatsoever. Accordingly, dependent claims 40-44 are allowable at least for those reasons previously of record.

II. Conclusion

In view of the foregoing remarks, Applicant respectfully submits that all of the claims of the present application are in condition for allowance. It is respectfully requested that a Notice of Allowance be issued in due course. Examiner Sax is encouraged to contact Applicant's undersigned attorney to resolve any remaining issues in order to expedite examination of the present application.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,

/Cory C. Davis/

Cory C. Davis
Registration No. 59,932

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street,
Suite 4000
Charlotte, NC 28280-4000
Tel Atlanta Office (404) 881-7000
Fax Atlanta Office (404) 881-7777

ELECTRONICALLY FILED USING THE EFS-WEB ELECTRONIC FILING SYSTEM OF THE UNITED STATES PATENT & TRADEMARK OFFICE ON March 5, 2008.